



Rec'd PCT 26 JAN 2005

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
5 février 2004 (05.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/012372 A3

(51) Classification internationale des brevets⁷ : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2003/002364

(22) Date de dépôt international : 25 juillet 2003 (25.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/09475 26 juillet 2002 (26.07.2002) FR

(71) Déposant (pour tous les États désignés sauf US) : GEM-
PLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activ-
ités de Gémenos, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : CORON,
Jean-Sébastien [FR/FR]; 4 rue Léon Delagrangue, F-75015
Paris (FR). JOYE, Marc [BE/FR]; 19 rue Voltaire,
F-83640 Saint Zacharie (FR). NACCACHE, David
[FR/FR]; 7 rue Chaptal, F-75009 Paris (FR). PAILLIER,
Pascal [FR/FR]; 37 Cours de Vincennes, F-75020 Paris
(FR).

(74) Mandataire : NONNENMACHER, Bernard; C/O Gem-
plus, Service Brevets, La Vigie, BP 90, F-13705 LA Ciotat
Cedex (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,
SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale

(88) Date de publication du rapport de recherche
internationale: 21 mai 2004

En ce qui concerne les codes à deux lettres et autres abrégia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: DATA ENCRYPTION METHOD, CRYPTOGRAPHIC SYSTEM AND ASSOCIATED COMPONENT

(54) Titre : PROCEDE DE CHIFFREMENT DE DONNEES EN UTILISANT UNE FONCTION PROBABILISTIQUE DE SI-
GNATURE, SYSTEME ET COMPOSANT ASSOCIES

(57) Abstract: The invention concerns an encryption method, comprising a step which consists in formatting a clear message (m) with a formatting function (μ), and a step which consists in an exponentiation of the result of the preceding step using a public key (N, e) in accordance with the relationship $c = \mu(m)^e \bmod N$, c being an encrypted message, $\mu(m)$ being the result of the formatting step, and e and N elements of the public key. The invention is characterized in that the formatting function (μ) is The PSS function. The invention is applicable to cryptography, for example of RSA type, for smart cards for instance.

(57) Abrégé : L'invention concerne un procédé de chiffrement, comprenant une étape de formatage d'un message clair (m) par une fonction de formatage (μ), et une étape d'exponentiation du résultat de l'étape précédente à l'aide d'une clé publique (N, e) selon la relation $c = \mu(m)^e \bmod N$, c étant un message chiffré, $\mu(m)$ étant le résultat de l'étape de formatage, et e et N des éléments de la clé publique. Selon l'invention, la fonction de formatage (μ) est la fonction PSS. Application au domaine de la cryptographie, par exemple de type RSA, par exemple pour des cartes à puces.

WO 2004/012372 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/02364

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BELLARE M ET AL: "THE EXACT SECURITY OF DIGITAL SIGNATURES - HOW TO SIGN WITH RSA AND RABIN", ADVANCES IN CRYPTOLOGY - EUROCRYPT '96. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. SARAGOSSA, MAY 12 - 16, 1996, P. 399-416 XP000725449 ISBN: 3-540-61186-X cited in the application page 407, line 33 -page 409, line 14 --- -/--	4

☒ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

6 February 2004

Date of mailing of the international search report

13. 02. 2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Liebhardt, I

INTERNATIONAL SEARCH REPORT

International Application No

PO/FR 03/02364

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>BELLARE, M., ROGAWAY, P.: "Optimal Asymmetric Encryption - How to Encrypt with RSA"</p> <p>FULL VERSION OF THE PAPER THAT APPEARED IN THE PROCEEDINGS OF ADVANCES IN CRYPTOLOGY - EUROCRYPT '94, 19 November 1995 (1995-11-19), XP002238170</p> <p>page 2, line 1 -page 3, line 12</p> <p>---</p>	1-10
A	<p>HABER, S., PINKAS, B.: "Securely Combining Public-Key Cryptosystems"</p> <p>PROCEEDINGS OF THE ACM COMPUTER AND SECURITY CONFERENCE, November 2001 (2001-11), XP002238171</p> <p>page 215, left-hand column, line 1 - line 9</p> <p>page 221, left-hand column, line 58</p> <p>-right-hand column, line 11</p> <p>---</p>	1-10
P,X	<p>CORON J -S ET AL: "Universal padding schemes for RSA", ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2442), ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA , 2002, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 226 - 241 XP002265380</p> <p>ISBN: 3-540-44050-X</p> <p>the whole document</p> <p>-----</p>	1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Des. Internationale No

PCT/FR 03/02364

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
-------------	------------------------------------------------------------------------------------------------	-------------------------------

A	<p>BELLARE M ET AL: "THE EXACT SECURITY OF DIGITAL SIGNATURES - HOW TO SIGN WITH RSA AND RABIN", ADVANCES IN CRYPTOLOGY - EUROCRYPT '96. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. SARAGOSSA, MAY 12 - 16, 1996, P. 399-416 XP000725449 ISBN: 3-540-61186-X cité dans la demande page 407, ligne 33 -page 409, ligne 14</p> <p style="text-align: center;">---</p> <p style="text-align: center;">-/-</p>	4
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

6 février 2004

Date d'expédition du présent rapport de recherche internationale

13. 02. 2004

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Liebhardt, I

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/02364

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>BELLARE, M., ROGAWAY, P.: "Optimal Asymmetric Encryption - How to Encrypt with RSA" FULL VERSION OF THE PAPER THAT APPEARED IN THE PROCEEDINGS OF ADVANCES IN CRYPTOLOGY - EUROCRYPT '94, 19 novembre 1995 (1995-11-19), XP002238170 page 2, ligne 1 -page 3, ligne 12</p> <p style="text-align: center;">---</p>	1-10
A	<p>HABER, S., PINKAS, B.: "Securely Combining Public-Key Cryptosystems" PROCEEDINGS OF THE ACM COMPUTER AND SECURITY CONFERENCE, novembre 2001 (2001-11), XP002238171 page 215, colonne de gauche, ligne 1 - ligne 9 page 221, colonne de gauche, ligne 58 -colonne de droite, ligne 11</p> <p style="text-align: center;">---</p>	1-10
P,X	<p>CORON J -S ET AL: "Universal padding schemes for RSA", ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2442), ADVANCES IN CRYPTOLOGY - CRYPTO 2002. 22ND ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA , 2002, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 226 - 241 XP002265380 ISBN: 3-540-44050-X le document en entier</p> <p style="text-align: center;">-----</p>	1-10